Exhibit A: Statement of Work

In this Exhibit A, the City may be referred to as the “client” or as “Customer”.

Scope of Services

SERVICES SELECTED

The tables below specify the items included and level of service:

7x24x365 Proactive Device and Application Monitoring & Management

Monthly per Device Pricing

Device	Monitoring	Monitored & Managed
Cisco Application Server	$ 188.00	$ 561.00
Host	$ 188.00	$ 281.00
Gateway - PRI / SIP (Includes SRST)	$ 125.00	$ 200.00
Gateway - Analog	$ 125.00	$ 152.00

Devices Covered under the scope of this agreement:

Device	Qty	NCare Device Classification	Coverage Model
Call Manager	3	Cisco Application Server	Monitored and Managed
Unity	2	Cisco Application Server	Monitored and Managed
UCCX	2	Cisco Application Server	Monitored and Managed
IM&P	2	Cisco Application Server	Monitored and Managed
Informacast	1	Cisco Application Server	Monitored and Managed
Prime	1	Cisco Application Server	Monitored and Managed
Emergency Responder	2	Cisco Application Server	Monitored and Managed
UCS Server	2	Host Server	Monitored and Managed
Voice Gateway	2	Gateway - PRI/SIP	Monitored and Managed

Total Solution Pricing

Annual fee is calculated from the number and type of devices covered in the scope of the agreement in table above charged at the ‘Monitored and Managed’ level of service rate.

Service Description	One Time Enablement Fee	Annual Y1-Y5
NCare 24x7x365 Proactive Device Monitoring & Management	$9,800.00*	$99,060.00

SCOPE OF SERVICES

The following specifies the services that NWN will provide to CITY OF DURHAM:

DEVICE AND APPLICATION PROACTIVE MONITORING SERVICE

7x24 Monitoring and Multi-Tier Notification

With 7x24 device and application monitoring, NWN will monitor the client’s environment through the use of specially configured applications and tools installed at the 7x24 monitoring facilities at our Datacenter in Waltham, MA. NWN will monitor the status of the devices and be alerted to problems and potential problems. Thresholds will be set to trigger alarms for immediate, remedial response.

There are hundreds of attributes which are tracked and captured across the different devices NWN monitors. Examples of the types of attributes we capture for network UC devices include but are not limited to:

- CPU, Memory usage
- Environmental probes (POE, Fans, etc.)
- Up/Down of device
- Interface Utilization
- Interface errors
- Critical uplink interfaces up/down (Trunks)
- Interface throughput stats
- Bandwidth Utilization (firewalls and/or circuit facing interface)
- CTI device registration issues
- Voice Gateway registration issues
- PRI saturation and/or operational issues
- Issues with ICT or SIP trunking
- Critical OS services
- Disk space utilization

.

Incident Assessment and Escalation

System monitoring provides a significant amount of information which must be evaluated to determine if a true incident has occurred. As part of the incident assessment activity, alerts which the monitoring tools have created are evaluated for validity. NWN engineers will review these alerts 7x24 and determining if they are true incidents.

In addition to incidents which are identified through the monitoring tools, the initial incident assessment is applicable for incidents which are raised via a phone call, email, etc. These incidents will be assessed to determine their root cause. Through this activity they will either be resolved quickly or escalated appropriately depending on the service requirements.

7x24 Case Management Tool

Incidents identified and escalated are documented in an online case management system. NWN will provide access to this online system to City of Durham designated employees.

7x24 Online Monitoring Portal

As part of the monitoring solutions, the client has access to all CITY OF DURHAM monitoring information through an online portal. This information is provided both in a summary fashion as well as a drill down into the status and activities of a particular device.

Management of the monitoring tool

As part of the proactive monitoring, NWN will perform the initial enablement of the monitoring tool as well as the ongoing maintenance of the tool. This includes but is not limited to: reviewing the current threshold levels, making updates based on best practices and customer specific requirements and keeping the tool current to the latest revision.

Monthly analysis reports

On a monthly basis, the client will receive an analysis report of the critical information captured with regards to the client's environment along with a technical summary about the key statistics. These reports can be utilized to identify preventative maintenance activities as well as future planning on the technical direction for the network environment.

DEVICE AND APPLICATION PROACTIVE MONITORING AND MANAGEMENT

Note: Device and Application Proactive Monitoring and Management as outlined below include, in addition, all the services listed above in the Device and Application Monitoring section.

7x24x365 Engineering Support

NWN provides 7x24x365 support services as a foundation for our managed services contract. An Assigned Solutions Engineer responds to incidents 7x24x365 in order to best support your networking environment. NWN's Command Center will log, track, and prioritize incidents providing engineering support.

Incident Support

NWN focuses on supporting our customers IT Infrastructure. The scope of Network incidents which we will help our customer resolve includes:

Task	Supported
Incidence	
Hardware	✓
Operating System	✓
Configuration	✓
Performance	✓

Security	✓
Back-ups	✓
Messaging (if messaging device included in scope)	✓
IP Communication (if IPC device included in scope)	✓
Device Management	✓

Examples of the types of Network and UC issues we will help resolve include:

- Environmental sensor threshold breached
- Hardware issues
- IOS stability
- Voicemail issues
- Server and Application issues
- Station (phone) issues
- Trunk issues
- CDR outage issues
- System backup issues
- System timing/clock issues

Incidents are escalated based on criticality. Criticality is defined as follows:

Criticality Level	Description
Priority 1 (Critical)	A critical system or service is unavailable.
Priority 2 (Major)	An issue has been detected where functionality is interrupted however there is either a work-around or the service interruption is occurring on a non-critical system or service.
Priority 3 (Minor)	The functionality of a non-critical system or service has been affected. An error has been detected that is easily corrected or is identified as a non-reoccurring or spurious.

Examples of priority 1 UC issues:

- Voice Gateway outage
- Server/Application down
- Entire site inbound/outbound dialing issues

Should a Priority 1 issue be identified, NWN will focus an engineer or team of engineers to fix the problem.

Vendor escalation will many times be immediate. Vendor involvement shall be agreed upon by both the City and NWN staff based time on constraints and the criticality of the situation. An example of Vendor escalation is:

- For a device (network device, application server, etc.) down where we identified a hardware failure, NWN would escalate to Cisco for RMA and coordinate with onsite resources to replace the faulty device. The

Customer will be notified via the NWN case management system as well as the ASE/CDM provides the customer with regular status updates.

For Priority 2 and Priority 3 situations, the City and NWN will agree upon an action and escalation plan based upon criticality and resource availability.

The City will designate a list of authorized callers that NWN will validate for security purposed upon opening a new case. It is the City's responsibility to notify NWN should this contact list change. Notifications should be emailed and all urgent changes should be followed up via a phone call to the command center.

NWN maintains support escalation contracts with Cisco, Microsoft, HP, Novell, Citrix, and Symantec. These contracts stipulate that NWN will act as 1st and 2nd level support. For all Priority 2 and Priority 3 issues, NWN staff will attempt remediation of issues. Should the issue not be solved within a reasonable amount of time, NWN will escalate calls to these vendors using its contracts. The City may request that all Level 1 calls be immediately escalated to these vendors.

NWN will work with other client vendors directly and will coordinate troubleshooting efforts over the phone. It is the client's responsibility to maintain all other vendor escalation contracts with their individual respective vendors. Many vendors require directly purchased support in order to provide 2nd and 3rd level support and code updates.

It is also the City's responsibility to ensure compliance with individual vendor's requirements regarding version supportability. Products that are no longer supported by their respective vendor will be supported by NWN on a "best-effort" basis. If NWN can obtain support for these products on a "for-fee" basis, NWN will seek approval for this additional support from the City and will pass all fees associated with such requests back to the City.

Scheduled Maintenance

Scheduled maintenance is defined as activities which are planned in advance to keep a network healthy. NWN will work with the City to determine the best time to perform scheduled maintenance. This type of support may be performed either remotely or on-site depending on the circumstances of the activity. Examples of potential schedule maintenance tasks depending on the device may include:

- Hosts
  - Quarterly Patching
  - Review Host Warning Alarms Regularly (Critical and Error are automatically escalated as incidents)
  - Hardware Warranty Check
  - Identify the method of backups and status
- UC Application Servers
  - Reviewing Health and Performance Stats from monitoring systems
  - Quarterly patching (ex. 9.1.2(SU3) to 9.1.2(SU4)
  - Verify backups and remediate any issues
  - Station firmware updates as needed (vulnerability remediation, bugs, etc.)
- Voice Gateways
  - Reviewing Health and Performance Stats from monitoring systems
  - Annual patching (ex. 15.2T(M4) to 15.2T(M7)
  - Additional patching/updates as necessary (Security Advisories, Bugs, etc.)
  - Backups of configurations

Functional Change request

A functional change request is defined as a request to change the operation of a device that is being managed in production. These requests typically come in the form configuration changes to the device. Functional Change requests are submitted by the client through the on-line customer portal or emailed. They are reviewed, assessed, approved, scheduled and executed as part of the standard processes. All functional change requests are tracked within our ticketing system. The levels at which NWN will perform network functional changes include:

Task	Supported
Functional Change Requests	
Configuration	✓
Minor call flow updates (patterns, CSS, partition)	✓
UCCX skills, resources and triggers	✓
Bulk Administration of devices, users, profiles, voicemail boxes etc.	✓
Dial Peers, translation patterns, etc.	✓
Operating System	✓
IOS Updates	✓
Security Advisories	✓

Change Management

NWN uses ITIL best practices and will conform to the customer's change management process as agreed upon. NWN will utilize NWN's Change Control System within their ServiceNow to document changes.

NWN's standard Change Management process is as follows:

1) Accept Request

The request is completed by NWN or the client. Work is accepted by ASE.

2) Complete and Submit Change control request

Submit request for review by customer during regular change control meeting. Requests at a minimum should include:

- Potential impact of change (from user perspective)
- Detailed change procedure
- Back-out plan if change is unsuccessful
- Test plan to make sure environment is not impacted and change is complete
- A proposed schedule and change control window for the change (during regular change windows set during enablement process unless change is an emergency)

3) Change Control Meeting – Customer Acceptance

A regular meeting is held to discuss active change controls. In this meeting the customer approves, approves with modification, or rejects the change control request. If rejected, the request may be reworked and sent back to 14.2 or discarded/cancelled.

4) Execute Change

Change is executed. If the change falls out of the approved window, it must be backed out unless the client explicitly extends the window.

5) Test

The change is tested for completion and for potential adverse impact to the environment and the users. Determination is made whether to back the change out.

6) Back Out Change

The change is backed-out as documented in the change control request.

7) Client Notification

The City is notified of the results of the change.

Monthly Management Reporting

Tracking and reporting are key components of the support services. On a monthly basis, NWN will provide a summary report of the work performed on the customer's behalf. This will include:

- Monthly Bandwidth Analysis
- Proactive Maintenance Reporting
- Incidents
- Scheduled Maintenance
- Functional Change Requests
- SLA Reporting

Monthly Incident reporting

Incidents are captured in the ticketing system. On a monthly basis a snapshot is taken of what incidents have been completed over the course of the month as well as what incidents are currently outstanding. This information is included as part of the monthly summary report.

Monthly Scheduled Maintenance reporting

Scheduled Maintenance activities are captured in the ticketing system. On a monthly basis a snapshot is taken of what scheduled maintenance has been completed over the course of the month as well as what schedule maintenance is currently outstanding. This information is included as part of the monthly summary report.

Monthly Change request reporting

Functional Change requests are captured in the ticketing system. On a monthly basis a snapshot is taken of what functional change requests have been completed over the course of the month as well as what functional change requests are currently outstanding. This information is included as part of the monthly summary report.

7x24 Online Ticket Creation and Status

7x24 online access to the NWN ticketing system enables customers to both create new tickets and find out the status of an existing ticket. When tickets are created, they are immediately routed to our command center engineers who are available 7x24. These tickets will be reviewed and addressed appropriately depending on the priority and level of service required.

In addition, any time day or night you can check the status of an existing ticket. Find out where it is in the work cycle, who it has been assigned to and what work has been accomplished to date.

Tickets may also be created via email.

GENERAL SERVICES INCLUDED

Solution Engineer Assigned to Account

A solution engineer is a level 2 engineer with a broad set of experiences. Both a primary and backup solution engineer, with a deep level of expertise in the type of architecture, hardware, software, and functionality in your specific configuration is assigned to your environment to facilitate a deeper understanding of your environment to assist in troubleshooting issues and providing valuable analysis reports of your network infrastructure. Also, they represent an additional point of contact into the managed services organization and a single point of escalation.

Customer Delivery Manager Assigned to Account

NWN will assign a Customer Delivery Manager (CDM) to take ownership for all activities associated with the client account. The key metric of their success is the customer satisfaction ratings provided by the client as part of the annual operations assessment. Their role will be to manage the functional change request process, customer communications and be the customers advocate.

Annual Operational Assessment

NWN works to go beyond the tactical day-to-day support services, and include an annual operational assessment on managed devices.

During the course of ongoing monitoring, support, and maintenance, work is performed and problems are solved on a tactical level. The annual assessment process is designed to ensure tactical IT Operations are in sync with strategic business goals and objectives. The annual assessment will be conducted not more than 12 months after the beginning of the engagement and annually thereafter for the term of the SOW.

Key components of the Annual Operations Assessment include:

- Match business challenges to potential Technology Solutions
- Review and adjust existing levels of support. Create action plans for improving level of support and value.
- Provide feedback on new and emerging technologies and trends
- Discuss effectiveness and satisfaction with NWN's services
- Improve NWN's understanding of the client's Business and internal Processes
- Understand the Risks and Impact to the Organization related to technology options
- Understand the Financial Metrics of technology choices

The Custom Delivery Manager and Solution Engineer will meet with the Customer and review the Annual Operations Assessment and make changes as agreed upon during the meeting.

SERVICE LEVEL AGREEMENTS

Service Levels will be calculated and reported monthly, and measured quarterly. Service Levels apply to support tasks based on priority and applicable NCare service. Priorities are defined as follows:

Priority Level	Definition for Monitoring & Management Support Services
Priority 1	• A critical system or service is unavailable, causing a severe impact on operations. There is no alternative, redundant or back-up to this system or service.
Priority 2	• A critical system or service is slowed or interrupted, however a work-around is in place so that operations can continue. • A service interruption is occurring on a non-critical system or service.
Priority 3	• The functionality of a non-critical system or service has been degraded. • An error has been detected that is not affecting service performance or availability.

Service	Service Level Agreement
Network Operations Center (NOC)	
• Availability: Support Staff	NWNs Network Operations Center will be staffed 7 X 24 X 365
• Response: Speed of Answer	90% of calls will be answered within 60 seconds.[1]
• Response: Abandonment	Less than 3% after 60 seconds.[2]
• Response: Email	Cases will be created with 15 minutes of email arriving in NWN Case management system.
Management Services	
• Incident support	Incidents within NWN's control will be resolved within the following timeframes (80%).[3] • Priority 1 – 4 hours • Priority 2 – 2 business days • Priority 3 – 3 business days
• Scheduled maintenance	Scheduled maintenance will be completed within the following timeframes (80%) after customer authorization.[4] • Priority 1 – 2 business days • Priority 2 – 5 business day • Priority 3 – 10 business days

[1] Measured Monthly across all clients

[2] Measured Monthly across all clients

[3] Does not include time spent waiting for action outside of NWN control, Reporting period must contain a minimum of 10 case per priority

[4] Does not include time spent waiting for action outside of NWN control, Reporting period must contain a minimum of 10 case per priority

• Functional change request	Functional change requests completed within the following timeframes (80%) after customer authorization.[5] • Priority 1 – 2 business days • Priority 2 – 5 business day • Priority 3 – 10 business days
• MACD (Move/Add/Change/Delete) request	MACD requests completed within the following timeframes (80%) after customer authorization.[6] • Priority 1 – 2 business days • Priority 2 – 5 business day • Priority 3 – 10 business days (80%) after customer authorization
Monitoring Services	
• 7x24 device monitoring and notification	• Incidents will be identified within the following parameters (90%)[7] ○ Priority 1 – 30 minutes ○ Priority 2 – 60 minutes ○ Priority 3 – 24 hours NWNs case tracking system will send confirmation of case creation via email within 1 hour 99%
• 7x24 Online Monitoring Portal	• Online monitoring portal available 7x24x365 (99.5%) excluding scheduled maintenance.
• Monitoring	• NWN will monitor devices 99.5% excluding schedule maintenance outages for monitoring system
Reporting	
• Monthly reporting	• Monthly reporting will be delivered within 10 business days of the end of the reporting period for services that include monthly reporting

[5] Does not include time spent waiting for action outside of NWN control, Reporting period must contain a minimum of 10 case per priority

[6] Does not include time spent waiting for action outside of NWN control, Reporting period must contain a minimum of 10 case per priority

[7] Identification is defined as time from incident occurrence to ticket creation. Identification is a team effort between NWN and the Customer. Our experience is that for certain types of issues, users may discover the problem before our remote monitoring tools can highlight the problem to us.

Assumptions and Terms

- The contract term is for five years beginning on the date of acceptance.
- Billing:
  - Enablement fees, if applicable, will be billed in full at the initiation of the enablement process after signing of the contract.
  - Annual services fees will be invoiced quarterly thirty (30) days prior to the start of each quarter.
- Incremental additions, changes and deletions to device counts can be executed via a written change order to this contract and billing changes will affected at the next billing cycle. The price per device per month when calculating charges is as follows:

Device	Monitoring	Monitored & Managed
Cisco Application Server	$ 188.00	$ 561.00
Host	$ 188.00	$ 281.00
Gateway - PRI / SIP (Includes SRST)	$ 125.00	$ 200.00
Gateway - Analog	$ 125.00	$ 152.00

- CITY OF DURHAM will provide "smart hands" for any remote assistance needed.
- This contract may be cancelled before the end of the contract term with 3 months written notice. After the three month notice, NWN will assess a 10% cancellation fee for the remaining months of the contract year.
  - Example: Contract termination at 7 months into the contract year would result in a 10% on the remaining 5 months. $8255/ month Service fee * 5 months* 10% = $4127.50 Cancellation Fee
  - This fee will be waived if cancellation is due to dissatisfaction that NWN cannot address including but not limited to failure to meet service level agreements specified in this Exhibit A: Statement of Work.
- For Monitoring Support: The client will provide space, power, network and internet connectivity for each monitoring server needed for the scope of the contract. NWN will provide the hardware and software for the monitoring server.
- The scope of services as specified herein applies to maintaining a healthy production environment. Upgrades to the environment or the implementation of new technology would be considered outside the scope of this contract and shall be treated as a project for which services may be contracted separately.